BGPKIT RESEARCH NOTE

A 2026 BGP hijack campaign against Chinese ISPs

From forged origins to forged paths, June to October

Mingwei Zhang, mingwei@bgpkit.com November 6, 2026, data through 20:43 UTC

Between June 10 and October 14, 2026, AS402425 and AS198474 used two techniques against Chinese ISP address space. From June 10 to July 7 they forged origins on 13 /24s inside China Mobile, China Unicom, and China Telecom space, in bursts of minutes. From July 19 they forged AS paths instead, placing AS402425 above real carrier origins: six China Unicom prefixes, then 1,294 China Mobile prefixes on August 1, then a fixed set of 225 that shrank to 76 and was last seen on October 14. The first technique worked where no ROA existed; the second left the origin untouched, so origin validation had nothing to check. This report reconstructs both phases from public BGP archives, measures the origin phase at five-minute resolution, gives a daily 00:00 UTC snapshot series for the path phase, and states where the data stops.

At a glance

- **Two techniques, one campaign.** Phase one forged origins from June 10 to July 7. Phase two forged paths from July 19: a probe on six China Unicom prefixes, 1,294 China Mobile prefixes on August 1, a plateau of 223 to 225 through September 9, 76 from September 29, and nothing after October 14.
- **The pivot is the story.** Origin validation never caught phase one, because the targets had no ROAs. Phase two made it irrelevant: the origin was real and only the provider edge was forged.
- **Scale changed by two orders of magnitude.** Phase one announced 13 /24s of 256 addresses each; phase two opened on July 19 with six China Unicom aggregates, about 1.44 million addresses, peaked on August 1 at 1,294 prefixes, and ended on October 14 at 76.
- **The carrier changes with the phase.** IPTP carried the June origin bursts and the July 19 probe, while the July 6 burst went through peers at the Singapore IXes; six upstreams carried the August 1 scale-up, Converge among them; from August 18 to October 14 a single carrier, Cogent, carried everything that was left.
- **Unmeasured.** Traffic volume, DNS manipulation, and attribution sit outside this data.

Scope and limits, read before quoting

- **Hijack means unauthorized routing state.** The word describes what was announced, not the intent behind it.
- **Control plane only.** We report what collector peers received, not what end users experienced.
- **Sampling, not a survey.** The origin phase is replayed at five-minute resolution on 12 days; the path phase is a daily snapshot series. Both series give lower bounds on prefix counts and duration.

1 Why this campaign, and why now

On October 20, 2026 CNCERT published a report on gambling-site redirects in several Chinese provinces. It places the domain tampering inside AS402425 and refers to forged origin prefixes and forged AS sets registered in Internet routing registries [1]. On November 6, 2026 Doug Madory of Kentik described the same AS as a suspected front for a North Korean group and recommended de-peering [2].

Neither statement publishes prefixes, timestamps, or AS paths. A third analysis, published on September 18, 2026, describes two hijacks of 2026, divides this one into four phases, and counts up to 23,000 prefixes behind forged paths [3]. Section 5 explains why our own count is far smaller. This note does three things the published accounts do not: it measures the origin phase at five-minute resolution, it gives a daily series for the path phase from June to November, and it separates what each phase can and cannot prove.

2 Method: two filters, and why one was not enough

Bottom line. An origin filter answers “who announced this.” A path filter answers “who was placed upstream of it.” The campaign used one technique and then the other, so a report built on the first filter alone ends three months early.

- **Origin filter.** Announcements whose origin ASN is AS402425 or AS198474, the two announcing ASNs, across all prefixes. This is what any origin-hijack watch does.
- **Path filter.** An AS-path regular expression matching the two ASNs anywhere in the path. This is what catches a forged provider edge, where the origin stays legitimate and only the relationship is invented.
- **Sources.** RIS (`rrc00`, `rrc23`) and RouteViews (`route-views.sg`) via the BGPKIT Broker: RIB snapshots for daily state, five-minute update files for exact timing. RPKI history from the BGPKIT ROA archive, registration from ARIN and RIPE RDAP, IRR from RADB.
- **Windows.** Origin phase: every five-minute file on 12 days, plus hourly sampling from June 1 to August 1 and September 1 to November 6. Path phase: one snapshot per day at 00:00 UTC from June 10 to November 6, 150 snapshots in all. Hourly sampling caught 26 active days in phase one; 14 of them fall between 8-hour RIB snapshots and a poll at that cadence would have missed them.

The method is itself a finding: both filters are cheap to run and neither is new, and a campaign that switches technique is missed by whichever one an operator happens to run.

3 The two ASNs and the prefixes they originated

Bottom line. The two ASNs originated 16 prefixes in the window. Two are leased space with matching ROAs, 13 are /24s inside Chinese ISP aggregates with no ROA, and one is a British company’s space announced without authorization. The path prefixes in phase two belong to real Chinese carriers and are counted in Section 5.

	AS402425	AS198474
Registry	ARIN, QLL-AS-001, QOREXA LABS LLC, Ocean City NJ	RIPE, sponsored by ORG-CR158-RIPE
Registered	April 9, 2026 (org), April 17, 2026 (autnum)	April 23, 2026
Presence	Equinix Singapore (Jul 2), HKIX (Oct 27), SGIX (Nov 3); PeeringDB 42450	no PeeringDB record
Published IRR set	`AS402425:AS-CUSTOMERS` and `AS402425:AS-CONE` both list AS198474	member of both; also publishes `AS198474:AS-ALL`, whose members are six China Mobile ASNs
Today	`2.27.171.0/24`, invalid against today’s only covering ROA	`82.41.19.0/24`, intermittent, invalid

Table 1: The two announcing ASNs. The AS sets are maintained under `MAINT-AS402425` and carry remarks saying they exist for IRR-based prefix filtering, and were created in August and September 2026, after the origin phase. Sources: ARIN and RIPE RDAP, RADB, PeeringDB, RIS.

Prefix	Origin	First seen	Registry holder of the covering space
`45.202.46.0/24`	both, in sequence	Apr 30, 2026	AFRINIC, registrant QOREXA LABS; ROAs for AS17561, AS198474, AS402425
`2.27.171.0/24`	both	May 15, 2026	Ace Data Centers, `2.26.0.0/15`; campaign-time ROAs named both ASNs
`117.180.191.0/24`	AS402425	Jun 10, 2026	AS9808 China Mobile, `117.128.0.0/10`
`163.177.91.0/24`	AS402425	Jun 10, 2026	AS17816 China Unicom Guangdong, `163.177.0.0/16`
`219.128.130.0/24`	AS402425	Jun 10, 2026	AS4134 China Telecom, `219.128.0.0/13`
`219.128.128.0/24`, `.129`, `.131`, `.132`	AS198474	Jul 6, 2026	AS4134 China Telecom, `219.128.0.0/13`
`27.40.0.0/24`	AS198474	Jul 6, 2026	AS17816 China Unicom Guangdong, `27.40.0.0/13`
`58.247.118.0/24`, `112.64.143.0/24`, `112.65.184.0/24`	AS198474	Jul 6, 2026	AS17621 China Unicom Shanghai
`218.107.49.0/24`	AS198474	Jul 6, 2026	AS17622 China Unicom Guangzhou
`180.108.0.0/24`	AS198474	Jul 6, 2026	AS4134 China Telecom, `180.96.0.0/11`
`82.41.19.0/24`	AS198474	intermittent	`82.41.0.0/16`, Digital IT Creations (GB); covering ROA names AS834

Table 2: Every prefix the two ASNs originated in the window. Inside `219.128.128.0/22` the four /24s were split between the two ASNs: `.128`, `.129`, and `.131` by AS198474, `.130` by AS402425. `.132` sits just outside that /22.

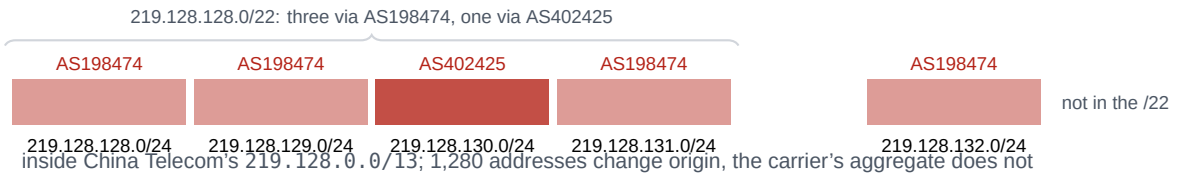


Figure 1: One /22, two origins. All four /24s of `219.128.128.0/22` were announced in the same campaign, three by one ASN and one by the other, plus a fifth immediately outside it.

4 Phase one: forged origins, June 10 to July 7

Bottom line. 13 /24s inside three Chinese carriers, announced by AS402425 and AS198474, in bursts of minutes across 26 days. None of them had a ROA, so origin validation had nothing to reject.

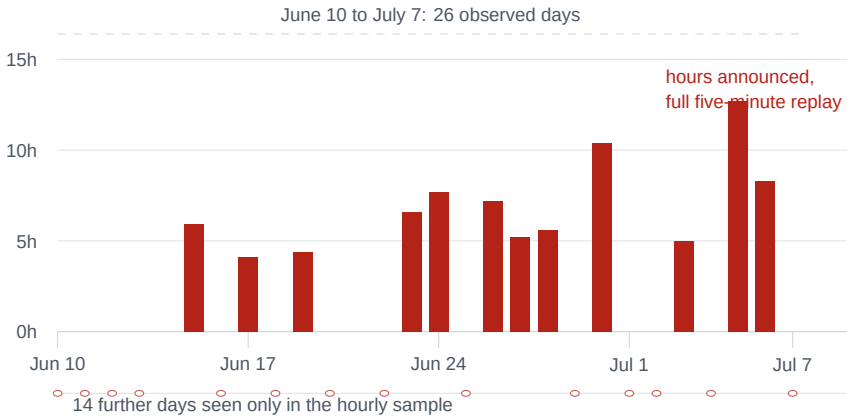


Figure 2: Phase one. Bars are total announced hours on the 12 days replayed at five-minute resolution; hollow markers are the 14 further days that hourly sampling catches and an 8-hour RIB census does not.

The mechanics are the familiar more-specific case: a /24 inside a live aggregate, a legitimate aggregate left in place, and the more specific winning wherever it was accepted. In the 16:00 UTC snapshot on June 15, all five prefixes AS402425 originated appeared at three collectors over about 20 distinct paths, every one through IPTP: its three Chinese /24s and the two leased /24s from Table 2. No other origin announced those /24s in that snapshot.

The phase takes two shapes. Across the 26 days, AS402425 announced its three Chinese /24s through IPTP in bursts of minutes. On July 6 the other ASN took over: AS198474 originated the ten /24s with AS402425 one hop above it, arriving through peers at the Singapore IXes, for example `133210 402425 198474`. That burst ended at 19:36:14 UTC, when both ASNs stopped in the same second. The ten /24s were still up in the July 7 snapshot, no longer through those peers but through `AS6939` and other transit, and July 7 is the last day the phase appears in our samples.

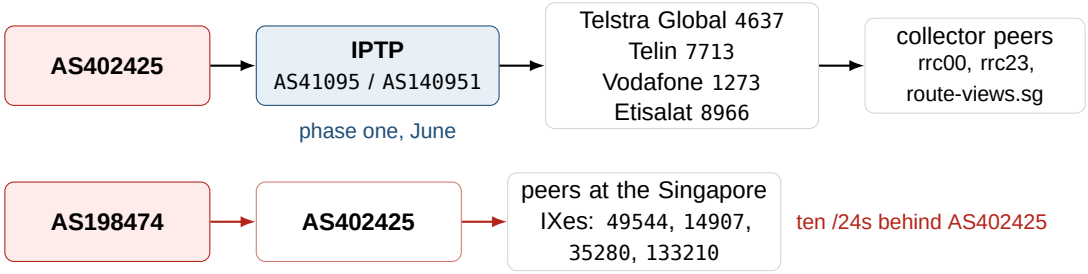


Figure 3: Two path shapes from the origin phase. Above: June, where AS402425 is the origin behind IPTP. Below: July 6, where AS198474 announces the ten /24s and AS402425 sits one hop above it. Both shapes are answerable with an origin-ASN or prefix query. Section 5 shows the shape neither query sees: a real carrier origin with a forged edge above it.

Two numbers from the replay frame the phase, and Appendix A query 1 rebuilds them. The median announcement lasted 5.5 minutes and the longest single announcement by one peer was 138 minutes, while the aggregate time announced across the 12 replayed days reaches 83 hours. That is a campaign of many short bursts, not one sustained announcement. The whole phase moved 256 addresses per prefix.

5 Phase two: forged paths, July 19 to October 14

Bottom line. From July the origin stays legitimate and only the provider edge is invented. The first path we catch, on July 19, is `852 41095 402425 4837`: AS402425 inserted between IPTP and China Unicom, so the origin is a real carrier ASN and its validation verdict does not change.

The claim in that path is a provider relationship, not an origin. One peer, `AS852`, reported all six prefixes, and the hop below AS402425 is `AS4837`, China Unicom, which legitimately originates Unicom space. Origin validation inspects the origin and nothing else, so it returns the same verdict for these prefixes as it did before the announcement, and has nothing to reject.

The six prefixes are aggregates, not /24s: `112.80.0.0/13`, `122.192.0.0/14`, `123.138.0.0/15`, `36.248.0.0/14`, `58.240.0.0/15` and `60.28.0.0/15`, about 1.44 million addresses in total. Phase one moved 256 addresses per prefix; the first day of phase two moved aggregates.

No origin-based watch can see this, which is why the same archive that dates phase one precisely says nothing about the months that follow. Filtering on the path instead gives three dated episodes of one technique.

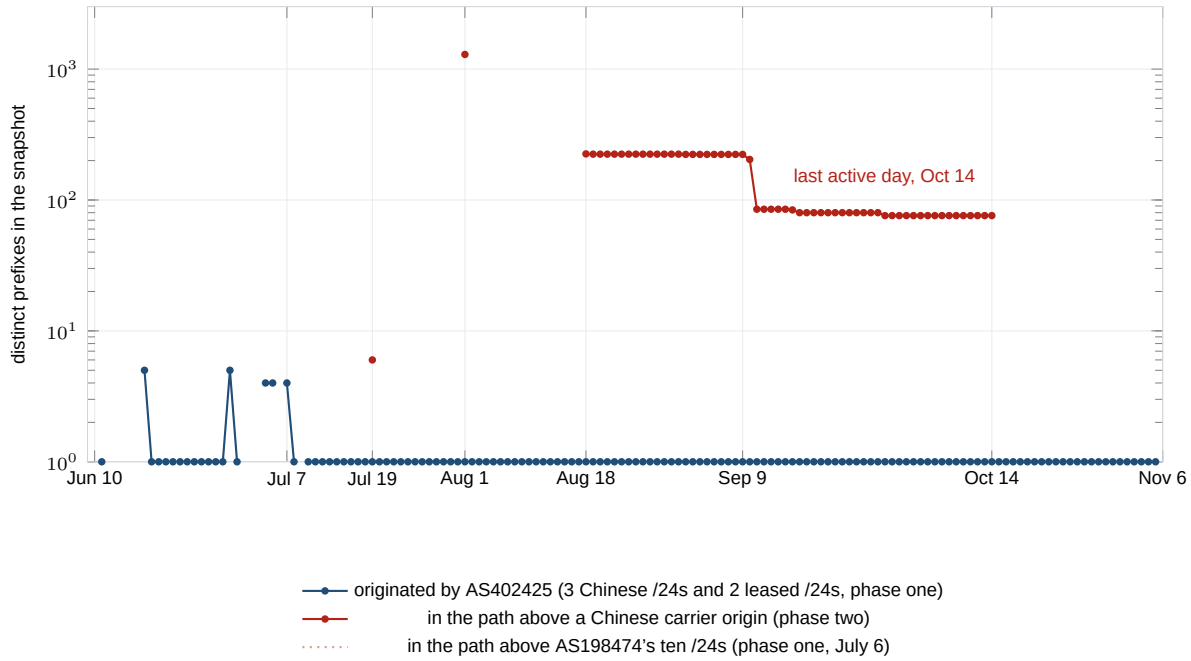


Figure 4: Daily series at `rrc00`, 00:00 UTC, log scale. Blue counts prefixes originated by AS402425, the dotted line counts the 10 /24s AS198474 originated on July 6, and red counts prefixes whose path contains AS402425 while the origin is one of the Chinese carriers. A gap means that snapshot showed none.

The red series is a sequence of discrete appearances, not a curve: 60 of the 150 daily snapshots carry it. The first episode is the July 19 probe just described. The second is a single day: August 1, when one snapshot carries 1,294 China Mobile prefixes. AS402425 stays the forged transit hop while the victim moves from China Unicom to China Mobile, and the real upstreams above AS402425 change too: that snapshot shows six at once, Converge `AS17639` carrying 1,294 prefixes, `AS38001` 1,292, `AS24482` 1,289, and `AS9930`, `AS8966` and `AS33891` below that.

The third episode starts on August 18 and lasts longest. The route returns with 225 prefixes, now through Cogent (`AS174`), and holds 223 to 224 a day until September 9. From September 10 it steps down: 204, then 85, then 80, then 76 at the end of the month. The plateau is one fixed set, not a rotation. Across the 23 days from August 18 to September 9 the union of the daily sets is exactly 225 prefixes, the same as the largest single day, and no day adds a prefix that August 18 did not already contain. What changes is only how many of that fixed set survive: 225, then 224, then the staircase down to 76. That contradicts the rotation the external analysis describes for the second half of August, at least at this collector and this hour. The end is abrupt and dated: 76 prefixes on every day from September 29 to October 14, then zero on October 15, and zero in every snapshot through November 6. These snapshots cannot tell whether the route was withdrawn, filtered upstream, or moved outside the 00:00 sample.

Snapshot, 00:00 UTC	Carrier-origin prefixes	Routes one hop above	Origin ASNs / carrier above
July 15, 2026	0	0	none
July 19, 2026	6	6	AS4837 China Unicom; AS41095 above
August 1, 2026	1,294	5,675	AS56046 and others; AS17639 above
August 10, 2026	0	0	none
August 18, 2026	225	569	AS56046; AS174 Cogent
September 9, 2026	223	316	AS56046; AS174 Cogent
September 10, 2026	204	210	AS56046; AS174 Cogent
September 14, 2026	85	85	AS56046; AS174 Cogent
September 28, 2026	80	80	AS56046; AS174 Cogent
October 14, 2026	76	76	AS56046; AS174 Cogent
November 6, 2026	0	0	none

Table 3: Selected rows from the daily series, one per plateau. Column two counts distinct carrier-origin prefixes with AS402425 in the path; column three counts `rrc00` peer-prefix routes that place AS402425 directly above the origin, so one prefix can contribute several.

An independent analysis of September 18, 2026 counts about 9,000 prefixes behind forged paths between July 25 and August 17, about 20,000 between August 18 and August 31, and 23,000 in its title, with Hurricane Electric carrying the scale-up and Cogent the rotation [3]. Those counts sit 7 to 18 times above our 1,294 in one snapshot, and need an explanation, because a reader who meets 13 /24s here and 23,000 there will assume one of the two numbers is wrong.

The three counts measure three different things. 13 is the number of distinct /24s whose origin was forged in phase one, so it counts address blocks, not announcements. 1,294 is the number of prefixes whose path carried AS402425 on August 1 while the origin stayed a China Mobile ASN, so it counts affected prefixes in one snapshot at one collector. The 9,000 and 20,000 are cumulative: every prefix seen behind a forged path at any hour and any collector in the stated window. Under that definition our own number would also exceed 1,294, because the union of every prefix seen across the 24 hours of a day is larger than any single snapshot of it.

We keep our definition because it is reproducible and because it fails in a known direction. What the comparison does establish is disagreement on two points that no definition can absorb: we never observe Hurricane Electric directly above AS402425 on a Chinese carrier path on any of the 60 active days, and we place the end later than their window, with 76 prefixes on every day from September 29 to October 14 and nothing from October 15 onward, six days before CNCERT published.

6 Why each phase beat the defense in front of it

Bottom line. Phase one is the only phase an origin check can catch. Phase two gives origin validation nothing to check, because the origin is real, and its episodes are the argument for path validation. No single control covers the campaign.

Control	Effect on this campaign	Where it acts
RPKI origin validation	Rejects phase one only if the targets have ROAs. They did not: all 13 returned NotFound, meaning no covering ROA. Phase two is unaffected because the origin is real.	Validating networks
IRR-based prefix filters	Rejects phase-one /24s that have no route object. In phase two the origins are the carriers' own, so the filter must come from the carriers' own objects; the attacker's AS sets, which name both ASNs and six China Mobile ASNs, are not a legitimate filter source for those origins.	Upstream and peers
Upstream filtering	Would remove an episode where it is applied: IPTP for June and the July 19 path event, Converge and other transit paths on August 1, Cogent from August 18. Each change of carrier moves the filtering point to another network, and these snapshots do not say whether filtering ended any episode.	One network per episode
ASPA (AS Provider Authorization) or path validation	The only control that addresses phase two, because it constrains which AS may appear as a provider. Coverage was 2.98% of origin ASNs on September 17, 2026 [3].	Validating networks
De-peering at exchanges	Local fabric only. A block at one exchange would have cut the July 6 burst, which arrived through peers there, but not the June bursts through IPTP or anything in phase two.	Local fabric
Detection	An origin watch sees phase one; a path watch sees the rest. Running only the first is how a four-month campaign gets recorded as a three-week one.	Monitoring

Table 4: Controls against the two phases, assessed against the paths we observed.

The conclusion is not that RPKI failed. It is that origin validation has nothing to say about a forged provider

edge, and the path technique ran for three months after the origin phase ended.

7 What it could affect

Bottom line. Phase one exposed 13 /24s of 256 addresses each. Phase two exposed up to 1,294 prefixes in a single snapshot, one hundred times more, and on its first day the aggregates it covered came to about 1.44 million addresses.

Where a network selected a forged route and does not validate, traffic toward those prefixes follows that route for as long as it lives: minutes in phase one, and in phase two for whatever the day's snapshot shows.

That is route selection, not a traffic measurement. It says where packets could have gone. It does not say how many did, and it does not speak to the DNS manipulation that CNCERT measured.

8 What third parties reported

Bottom line. Five external claims. Two restate the same official finding, one adds an injection location, one asserts attribution, and one gives a phase structure whose scale we cannot reproduce.

Source	Date	Claim	What it does not establish
CNCERT [1]	Oct 20, 2026	Tampering inside AS402425; forged prefixes and forged AS sets registered in routing registries; 19 malicious IPs; recommends revoking the AS	Prefixes, times, or how traffic was captured
CAICT via industry press [4]	Oct 27, 2026	Injection at Equinix Singapore; upstreams include Cogent and HE; Chinese operators blocked routes and flushed caches	A primary document
Kentik advisory [2]	Nov 6, 2026	Suspected front for a North Korean group; multiple hijacks in 2026; de-peer	Any published technical evidence chain
Wang analysis [3]	Sep 18, 2026	Four phases; 27 / 135 / 9,000 / 20,000 prefixes; HE then Cogent; path 1.38 hops shorter than legitimate	Reproducible per-day data
CGTN [5]	Oct 20, 2026	Restates CNCERT and notes the measurement does not establish intent	Not applicable; it is the caveat

Table 5: External claims and their limits. Our measurements add the prefixes, the daily series through November 6, and the two-filter method.

The CNCERT report refers to forged AS sets without naming any. What we can add is that three sets with these maintainers exist and were changed after the origin phase: `AS402425:AS-CUSTOMERS`, `AS402425:AS-CONE`, and `AS198474:AS-ALL`, whose members include six China Mobile ASNs. That they are the sets CNCERT meant is an inference, not a quotation. And the campaign end we can measure sits close to the report: the daily series carries China Mobile prefixes behind AS402425 until October 14 and nothing afterward, six days before CNCERT published.

9 Limitations

- **Path phase is a snapshot series.** One RIB per day at one collector, June 10 to November 6. A technique that runs for hours and stops is caught only if it overlaps 00:00 UTC on the day sampled.
- **Origin phase is sampled.** 26 days from hourly sampling, 12 of them replayed at five-minute resolution.
- **One collector for the series.** `rrc00` only; `rrc23` and `route-views.sg` confirm individual days but were not swept daily.
- **RPKI history.** The archive answers what was published on a date; an object published and withdrawn between daily snapshots is invisible.
- **No traffic data.** Every impact statement is about routing state.
- **Tooling caveat.** The BGPKIT historical validation endpoint returned wrong results for some prefix and date pairs before November 6, 2026; the defect is fixed and deployed.

Appendix A. Queries behind the numbers

The calls below rebuild the per-file and per-day facts. The sampling scans apply the same filters to every file in their stated window. Timestamps are Unix seconds.

```
# 1. origin-phase replay, one day, one prefix
monocle search -t 1781481600 -d 24h -D updates -c rrc23 \
  -p 117.180.191.0/24 -f prefix,as_path,peer_asn,timestamp

# 2. path-phase snapshot, one day
monocle search -t 1785542400 -d 1s -D rib -c rrc00 -a '.*402425.*' \
```

```
  -f prefix,as_path,peer_asn

# 3. origin census for either AS
curl -sG "https://stat.ripe.net/data/announced-prefixes/data.json" \
  -d "resource=AS402425" -d "starttime=2026-04-01T00:00:00" \
  -d "endtime=2026-11-06T23:59:59"

# 4. ROAs in force on a past date
curl "api.bgpkit.com/v3/roas/search?prefix=163.177.91.0/24&date=2026-06-15&exact=false"

# 5. current validation state
curl "stat.ripe.net/data/rpki-validation/data.json?resource=AS402425&prefix=2.27.171.0/24"
```

Appendix B. What was not measured. Traffic volume, DNS response contents, resolver logs, and user counts are outside every public BGP archive.

References

[1] CNCERT, *Investigation report on malicious tampering of DNS resolution data by overseas autonomous system AS 402425*, October 20, 2026. https://www.cert.org.cn/publish/main/upload/File/AS%20402425-report.pdf

[2] D. Madory, LinkedIn post on peering with Qorexa Labs (AS402425), November 6, 2026. https://www.linkedin.com/posts/dougmadory_psa-if-your-company-is-peering-with-qorexa-share-7524551937552252928-miwY/

[3] S. Wang, *Hetzner Impersonated, 23,000 China Mobile Prefixes Hijacked: Why Didn't RPKI Stop It?*, September 18, 2026. https://wangshuaizs.github.io/blog/posts/rpki-valid-hijacks-2026/en.html

[4] Industry summary of a CAICT security warning on AS402425, October 27, 2026. https://www.51dns.com/info/detail/14111.html

[5] CGTN, *Forged internet road signs send users to gambling sites*, October 20, 2026. https://news.cgtn.com/news/2026-10-20/Forged-internet-road-signs-send-users-to-gambling-sites-1RoKxbU32zS/p.html